Unit-15 Legal Aspects of Business - III

15.1 THE INFORMATION TECHNOLOGY ACT 2000

Introduction

- Information Technology Act 2000, is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.
- Information Technology Act 2000, is based on UNCITRAL (United Nations Commission on International Trade Law) Model Law.
- Information Technology Act 2000, has 13 chapters, 94 sections and 4 schedules.
    - First 14 sections deals with some legal aspects concerning digital signature.
    - Further other sections deal with certifying authorities who are licensed to issue digital signature certificate.
    - Sections 43 to 47 provide for penalties and compensation.
    - Sections 48 to 64 deals with Tribunals a appeal to high court.
    - Section 65 to 79 of the act deals with offences.
    - Section 80 to 94 deals with miscellaneous of the Act.

Objectives of the Act

The Information Technology Act, 2000 provides legal recognition to the transaction done via an electronic exchange of data and other electronic means of communication or electronic commerce transactions.

This also involves the use of alternatives to a paper-based method of communication and information storage to facilitate the electronic filing of documents with the Government agencies.

Further, this act amended the Indian Penal Code 1860, the Indian Evidence Act 1872, the Bankers' Books Evidence Act 1891, and the Reserve Bank of India Act 1934. The objectives of the Act are as follows :

(i) Grant legal recognition to all transactions done via an electronic exchange of data or other electronic means of communication or e-commerce, in place of the earlier paper-based method of communication.

(ii) Give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication

(iii) Facilitate the electronic filing of documents with Government agencies and also departments

(iv) Facilitate the electronic storage of data

(v) Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions

(vi) Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

Features of the Information Technology Act, 2000

(a) All electronic contracts made through secure electronic channels are legally valid.

(b) Legal recognition for digital signatures.

(c) Security measures for electronic records and also digital signatures are in place

(d) A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized

(e) Provision for establishing a Cyber Regulatory Appellant Tribunal under the Act. Further, this tribunal will handle all appeals made against the order of the Controller or Adjudicating Officer.

(f) An appeal against the order of the Cyber Appellant Tribunal is possible only in the High Court

(g) Digital Signatures will use an asymmetric cryptosystem and also a hash function

(h) Provision for the appointment of the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Controller to act as a repository of all digital signatures.

(i) The Act applies to offenses or contraventions committed outside India

(j) Senior police officers and other officers can enter any public place and search and arrest without warrant

(k) Provisions for the constitution of a Cyber Regulations Advisory Committee to advise the Central Government and Controller.

Scheme of I.T. Act

The following points define the scheme of the I.T. Act ?

- The I.T. Act contains **13 chapters** and **90 sections.**
- The last four sections namely sections 91 to 94 in the I.T. Act 2000 deals with the amendments to the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934 were deleted.
- It commences with Preliminary aspect in Chapter 1, which deals with the short, title, extent, commencement and application of the Act in Section 1. Section 2 provides Definition.
- Chapter 2 deals with the authentication of electronic records, digital signatures, electronic signatures, etc.
- Chapter 11 deals with offences and penalties. A series of offences have been provided along with punishment in this part of The Act.
- Thereafter the provisions about due diligence, role of intermediaries and some miscellaneous provisions are been stated.
- The Act is embedded with two schedules. The First Schedule deals with Documents or Transactions to which the Act shall not apply. The Second Schedule deals with electronic signature or electronic authentication technique and procedure. The Third and Fourth Schedule are omitted.

Application of the I.T Act

As per the sub clause (4) of Section 1, *nothing in this Act shall apply to documents or transactions specified in First Schedule. Following are the documents or transactions to which the Act shall not apply :*

- **Negotiable Instrument** (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
- A **power-of-attorney** as defined in section 1A of the Powers-of-Attorney Act, 1882;
- A **trust** as defined in section 3 of the Indian Trusts Act, 1882;

- A **will** as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;
- Any **contract** for the sale or conveyance of immovable property or any interest in such property;
- Any such class of documents or transactions as may be notified by the Central Government.

Amendments Brought in the I.T Act

The I.T. Act has brought amendment in four statutes vide section 91-94. These changes have been provided in schedule 1-4.

- The first schedule contains the amendments in the Penal Code. *It has widened the scope of the term "document" to bring within its ambit electronic documents.*
- The second schedule deals with amendments to the India Evidence Act. *It pertains to the inclusion of electronic document in the definition of evidence.*
- The third schedule amends the Banker's Books Evidence Act. *This amendment brings about change in the definition of "Banker's-book". It includes printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device. Similar change has been brought about in the expression "Certified-copy" to include such printouts within its purview.*
- The fourth schedule amends the Reserve Bank of India Act. *It pertains to the regulation of fund transfer through electronic means between the banks or between the banks and other financial institution.*

Intermediary Liability

Intermediary, dealing with any specific electronic records, is a person who on behalf of another person accepts, stores or transmits that record or provides any service with respect to that record.

According to the above mentioned definition, it includes the following ?

- Telecom service providers
- Network service providers
- Internet service providers
- Web-hosting service providers
- Search engines
- Online payment sites
- Online auction sites
- Online market places and cyber cafes

Highlights of the Amended Act

The newly amended act came with following highlights ?

- It stresses on privacy issues and highlights information security.
- It elaborates Digital Signature.
- It clarifies rational security practices for corporate.
- It focuses on the role of Intermediaries.
- New faces of Cyber Crime were added.

Digital Signature

A digital signature is a technique to validate the legitimacy of a digital message or a document. A valid digital signature provides the surety to the recipient that the message was generated by a known sender, such that the sender cannot deny having sent the message. Digital signatures are mostly used for software distribution, financial transactions, and in other cases where there is a risk of forgery.

Electronic Signature

An electronic signature or e-signature, indicates either that a person who demands to have created a message is the one who created it.

A signature can be defined as a schematic script related with a person. A signature on a document is a sign that the person accepts the purposes recorded in the document. In many engineering companies digital seals are also required for another layer of authentication and security. Digital seals and signatures are same as handwritten signatures and stamped seals.

Digital Signature to Electronic Signature

Digital Signature was the term defined in the old I.T. Act, 2000. **Electronic Signature** is the term defined by the amended act (I.T. Act, 2008). The concept of Electronic Signature is broader than Digital Signature. Section 3 of the Act delivers for the verification of Electronic Records by affixing Digital Signature.

As per the amendment, verification of electronic record by electronic signature or electronic authentication technique shall be considered reliable.

According to the **United Nations Commission on International Trade Law (UNCITRAL),** electronic authentication and signature methods may be classified into the following categories ?

- Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
- Those bases on the physical features of the user, i.e., biometrics.
- Those based on the possession of an object by the user, i.e., codes or other information stored on a magnetic card.
- Types of authentication and signature methods that, without falling under any of the above categories might also be used to indicate the originator of an electronic communication (Such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message).

According to the UNCITRAL MODEL LAW on Electronic Signatures, the following technologies are presently in use ?

- Digital Signature within a public key infrastructure (PKI)
- Biometric Device
- PINs
- Passwords
- Scanned handwritten signature
- Signature by Digital Pen
- Clickable "OK" or "I Accept" or "I Agree" click boxes

The faster world-wide connectivity has developed numerous online crimes and these increased offences led to the need of laws for protection. In order to keep in stride with the changing generation, the Indian Parliament passed the Information Technology Act 2000 that has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

The law defines the offenses in a detailed manner along with the penalties for each category of offence.

Offences

Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.

Cyber-crime usually includes the following :

- Unauthorized access of the computers
- Data diddling
- Virus/worms attack

- Theft of computer system
- Hacking
- Denial of attacks
- Logic bombs
- Trojan attacks
- Internet time theft
- Web jacking
- Email bombing
- Salami attacks
- Physically damaging computer system.

The offences included in the I.T. Act 2000 are as follows –

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Example

Offences Under The It Act 2000

Section 65. Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

Explanation : For the purpose of this section "computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Object : The object of the section is to protect the "intellectual property" invested in the computer. It is an attempt to protect the computer source documents (codes) beyond what is available under the Copyright Law

Essential Ingredients of The Section

knowingly or intentionally concealing

knowingly or intentionally destroying

knowingly or intentionally altering

knowingly or intentionally causing others to conceal

knowingly or intentionally causing another to destroy

knowingly or intentionally causing another to alter.

This section extends towards the Copyright Act and helps the companies to protect their source code of their programs.

Penalties : Section 65 is tried by any magistrate.

This is cognizable and non-bailable offence.

Penalties : Imprisonment up to 3 years and / or

Fine : Two lakh rupees.

The following table shows the offence and penalties against all the mentioned sections of the I.T. Act :

Section	Offence	Punishment	Bailability and Cognizability
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC.
66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs	Offence is Bailable and Cognizable
66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable and triable by Court of JMFC
66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-D	Cheating by Personation by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life	Offence is Non-Bailable, Cognizable and triable by Court of Sessions
67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form	On first Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non Bailable, Cognizable and triable by Court of JMFC

67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cybersecurity	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to 10 years and fine	Offence is Non-Bailable, Cognizable.
70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc., who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable
71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72-A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to Rs. 5 lakh.	Offence is Cognizable, Bailable
73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.

Compounding of Offences

As per Section 77-A of the I. T. Act, any Court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under the Act.

No offence shall be compounded if :

- The accused is, by reason of his previous conviction, is liable to either enhanced punishment or to the punishment of different kind; OR
- Offence affects the socio economic conditions of the country; OR
- Offence has been committed against a child below the age of 18 years; OR
- Offence has been committed against a woman.

The person alleged of an offence under this Act may file an application for compounding in the Court. The offence will then be pending for trial and the provisions of Sections 265-B and 265-C of Cr. P.C. shall apply.

Classification of Cyber Crimes

Cyber crimes are classified based on the subject of the crime, the person or organization against whom the crime is committed, and the temporal nature of the crimes committed online.

Based on the subject of the crime, cybercrimes are classified into three broad groups:

1. **Crimes Against Individuals :** These are committed against individuals or their properties. Some examples are:
   - Email harassment
   - Cyber-stalking
   - Spreading obscene material
   - Unauthorized access or control over the computer system
   - Indecent exposure
   - Spoofing via email
   - Fraud and also cheating
   - Further, crimes against individual property like computer vandalism and transmitting a virus. Also, trespassing online and intellectual property-related crimes. Further, internet time thefts are also included.
2. **Crimes Against Organizations :** Some examples of cyber crimes against organizations are:
   - Possessing unauthorized information
   - Cyber terrorism against a government organization
   - Distributing pirated software
3. **Crimes Against Society :** Some examples of crimes against society are:
   - Polluting the youth through indecent exposure
   - Trafficking
   - Financial crimes
   - Selling illegal articles
   - Online Gambling
   - Forgery

Apart from the ones listed above, crimes like hacking, denial of service attacks, e-mail bombing, etc. are also present in cyberspace.

Provisions of Cyber Crimes in the IT Act, 2000

The sections of the IT Act, 2000 pertaining to cybercrimes are as follows:

Section 43 : Penalty for damage to a computer, computer system, etc.

This section applies if any person, without the permission of the owner or the person in charge of a computer, system, or network -

- Accesses such computer, network or system.
- Copies, downloads or extracts any data or information from such computer, network or system (this also includes the information or data stored in a removable storage medium).
- Also, introduces or causes any computer containment or virus into such computer, network or system.
- Further, he damages any computer, system or data or any other programs residing in them.
- Disrupts or causes disruption of any such computer, system or network.
- Also, denies or causes the denial of access to an authorized person to such computer, system or network.
- Provides any assistance to anyone to facilitate access to such a computer, system or network contrary to the provisions of the Act and its rules.
- Also, charges the services availed of by one person to the account of another by tampering with such computer, system or network.

Penalty : Compensation, not exceeding one crore rupees to the affected person.

Section 65 : Tampering with the computer's source code documents

This section applies to a person who intentionally conceals, alters or destroys any computer source code used for a computer, program, system or network when the law requires the owner to keep or maintain the source code. It also applies to a person who intentionally causes another person to do the same.

Penalty : Imprisonment of up to three years or a fine of up to two lakh rupees, also both in some cases.

Section 66 : Hacking of a Computer System

This section applies to a person who commits hacking. Hacking is when the person intentionally or knowingly causes a wrongful loss or damage to the public or another person or destroys or deletes any information residing in a computer resource or diminishes its utility or value or injures it by any means.

Penalty : Imprisonment of up to three years or a fine of up to two lakh rupees, also both in some cases.

Section 67 : Publishing obscene information in an electronic form

This section applies to a person who publishes or transmits any obscene material – material which is lascivious or appeals to the prurient interests or tends to deprave or corrupt persons who are likely to read, see or hear the matter embodied in it. It also applies to a person who causes the publishing or transmission of such material.

Penalty : In case of the first conviction, imprisonment of up to five years and a fine of up to one lakh rupees. For subsequent convictions, imprisonment of up to 10 years and a fine of up to two lakh rupees.

Section 74 : Publication with the intention of fraud

This section applies to a person who knowingly creates, publishes or makes available a digital certificate with the intention of fraud.

Penalty : Imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases.

Other Provisions Relating to Cyber Crimes

Section 44 : Failure to furnish information, returns, etc.

This section applies to a person who

- Fails to furnish any document, return or report to the Controller or the Certifying Authority
- Fails to file returns or furnish any information as per the regulations or fails to furnish them in time
- Does not maintain the books of account or records

Penalty : The following penalties apply:

- A monetary fine of up to one lakh and fifty thousand rupees for each such failure
- A fine of up to five thousand rupees for every day if the failure continues
- A fine of up to ten thousand rupees for every day if the failure continues

Section 45 : Residuary Penalty

This section applies to a person who contravenes any rules under the IT Act, 2000, especially those for which there are no special provisions.

Penalty : A compensation of up to twenty-five thousand rupees to the affected person.

Section 71 : Misrepresentation

This section applies to a person who makes any misrepresentation to or even suppresses any material fact from the Controller or Certifying Authority to obtain the license or a digital signature certificate.

Penalty : Imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases.

Section 72 : Breach of confidentiality and privacy

This section applies to a person with secured access to any electronic record, information, or any other material, discloses it to another person without consent.

Penalty : Imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases.

Section 73 : Publishing a Digital Certificate with incorrect details

This section applies to a person who publishes a digital certificate with the knowledge that –

- The Certifying Authority listed in the certificate has not issued it
- The subscriber listed in the certificate has not accepted it
- It is a revoked or suspended certificate

Penalty : Imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases.

Section 74 : Publication with a fraudulent purpose

This section applies to a person who knowingly creates, publishes or makes available a digital signature for fraudulent purposes.

Penalty : Imprisonment of up to two years or a fine of up to one lakh rupees, also both in some cases.

Section 85 : Company Offences

(1) This section applies to a company who commits a contravention to the provisions of the Act. In such cases, all the people who were in charge and responsible for the company's conduct of business as well as the company are guilty of the contravention. Further, those responsible are liable for punishment. However, if a person is not aware of any such contravention, then he is not liable.

(2) Notwithstanding anything contained in the sub-section (1), if it is proved that the contravention was with the consent of, or due to the negligence of any director, manager or any other officer, then such people are also held liable.

For the purposes of this section, "company" means any body corporate and also includes a firm or other association of individuals.